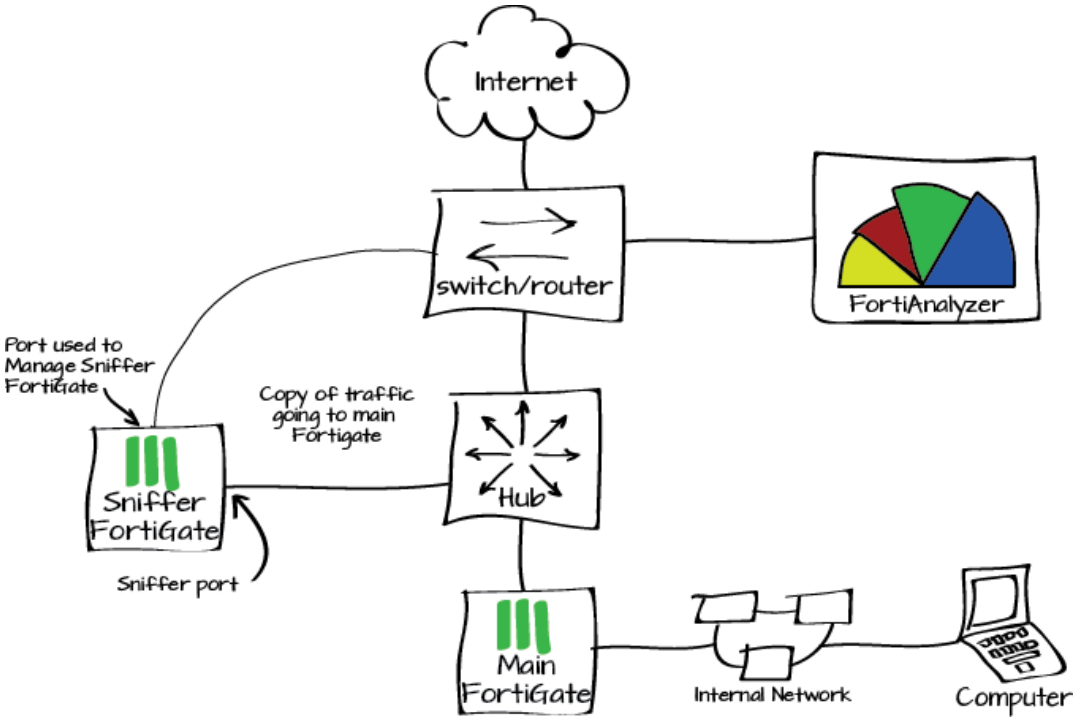
Analyzing your network traffic using a one-armed sniffer

You can use a one-armed sniffer in coordination with a FortiAnalyzer to analyze traffic going through a main FortiGate to minimize the impact on network performance impact.

Topology Setup

Sniffing can be done by way of port mirroring or by placing a hub between the FortiGate and the router/switch. Using a hub removes potential configuration issues with the switch.

1. Configuring the interfaces
2. Configuring the security profiles
3. Registering the sniffer device
4. Configuring logging to the FortiAnalyzer
5. Results



Configuring the interfaces

These settings are for the FortiGate designated as the “sniffer”; in this case a FortiGate model 60D.

It is possible to use the same interface for both the mirror traffic and access to the FortiAnalyzer, but it is recommended to use one for each purpose separately.

If there is not already administratively accessible interface, consider using FortiExplorer and a USB cable.

Configuring the Management Interface (WAN 1) on the Sniffer

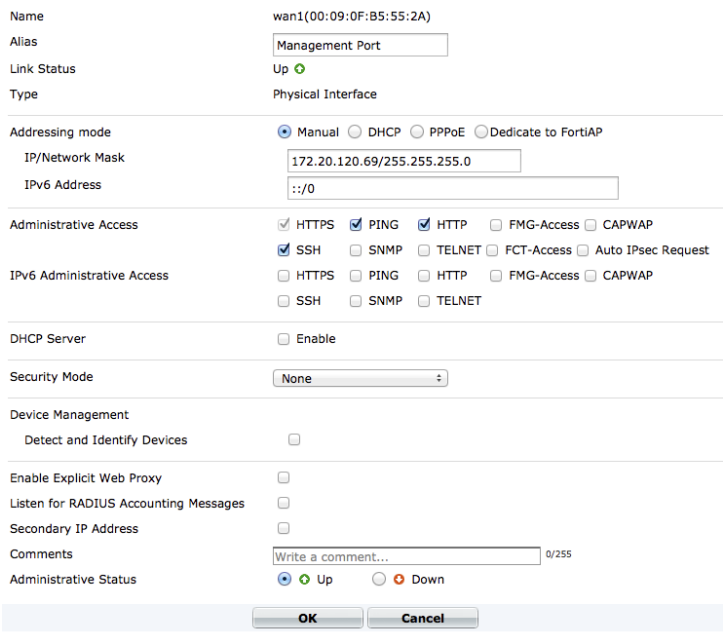
Log in to the FortiGate 60D.

Go to **System > Network > Interfaces**.

Select the interface that you wish to connect to your internal network so that you can access the device remotely and allow it to connect to the FortiAnalyzer.

Verify that the configuration for the interface is completed with the information shown here. Make sure that it is on the correct subnet range.

The purpose of this interface is to manage the FortiGate and provide access to the FortiAnalyzer so it is important to make sure that the correct **Administrative Access** is chosen and that the interface is on the internal subnet.

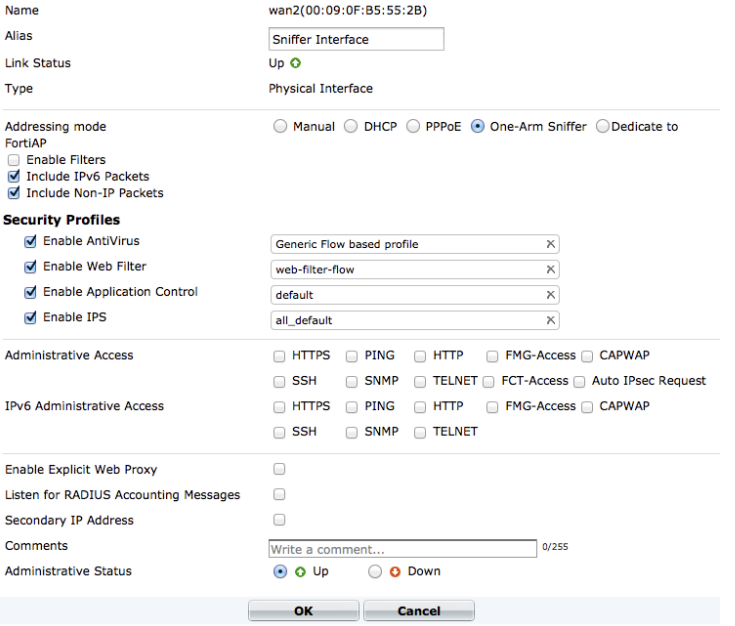


Configuring the sniffer interface

Select the interface that you wish to use to collect the mirrored data traffic.

Verify that the configuration for the interface is completed with the shown information:

If the One-Arm Sniffer addressing mode is unavailable you may have to choose a different interface.



Configuring the security profiles

Some administrators match the content of the profiles on the sniffer with those on the Main FortiGate, but this is not a requirement for the sniffer to work. The sniffer profiles will not impact your network performance so they can be as comprehensive as you want. Create profiles that will capture the information you want.

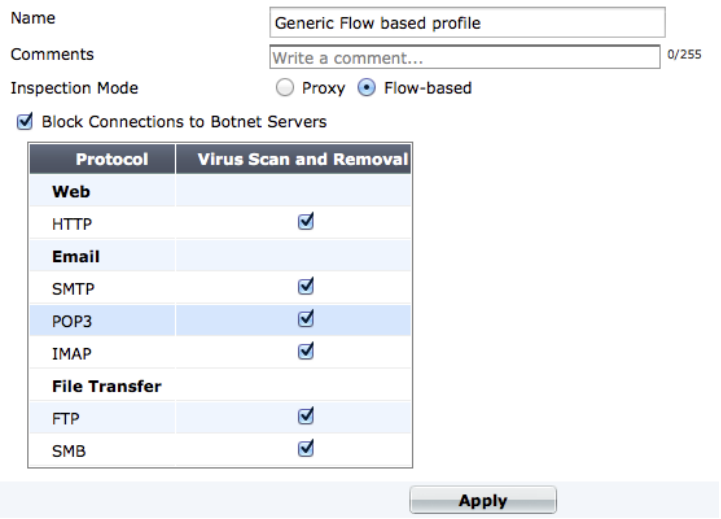
If you cannot set more than one type of Security Profile go to **System > Config > Features** and ensure that the **Multiple Security Profiles** feature is enabled.

AntiVirus Profile (Flow-based)

Go to **Security Profiles > AntiVirus > Profiles**.

Apply the same settings to the profile on the sniffer device as on the primary FortiGate.

The one-armed sniffer mode will only allow flow-based profiles to be used.



Configure the following in the CLI, in addition to the web-based configuration:

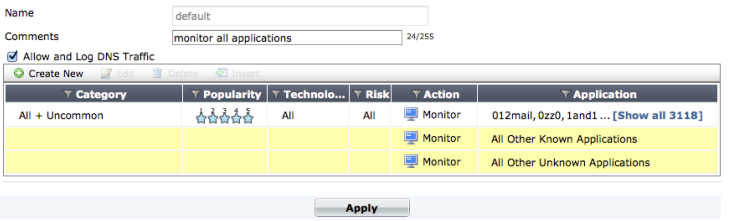
```
config antivirus settings
    set default-db normal
    end

config antivirus profile
    edit AV-flow
        set extended-utm-log enable
            config smb
                set options scan
            end
        set av-virus-log enable
        set av-block-log enable
    end
```

Application Control Sensor

Go to **Security Profiles > Application Control > Application Sensors**.

Apply the same settings to the profile on the sniffer device as on the primary FortiGate.



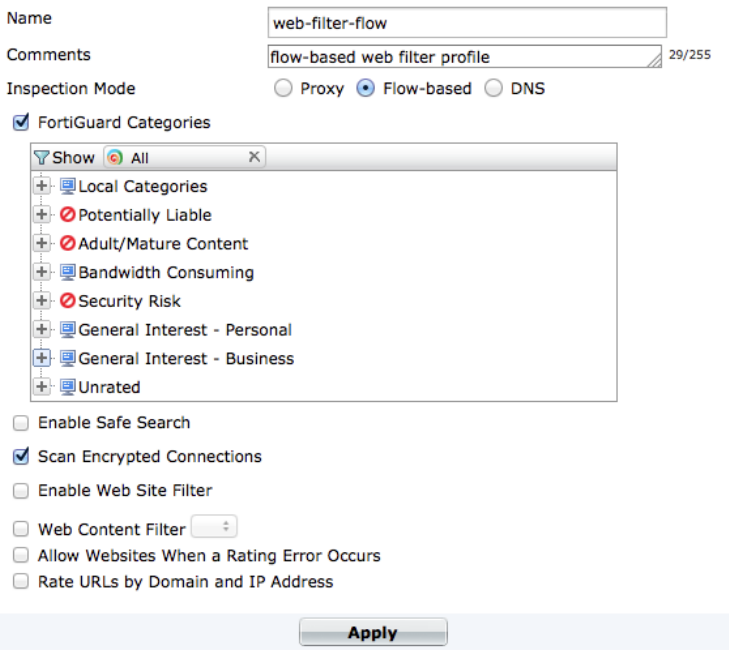
Add the these CLI settings in addition to the web-based configuration:

```
config application list
    edit "default"
        set extended-utm-log enable
        set other-application-log enable
        set log enable
        set unknown-application-log enable
    end
```

Webfilter Profile (Flow-based)

Go to **Security Profiles > Webfilter > Profiles**.

Apply the same settings to the profile on the sniffer device as on the primary FortiGate.



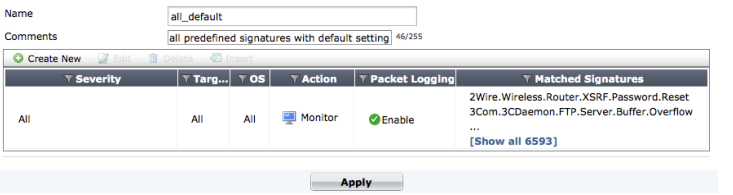
Configure the following settings in the CLI, in addition to the web based configuration:

```
config webfilter profile
    edit web-filter-flow
        set extended-utm-log enable
        set options https-url-scan
    end
```

IPS sensor

Go to **Security Profiles > Webfilter > Profiles**.

Apply the same settings to the sensor on the sniffer device as on the primary FortiGate.

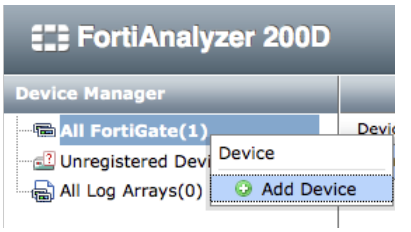


Registering the Sniffer device

Log in to the FortiAnalyzer.

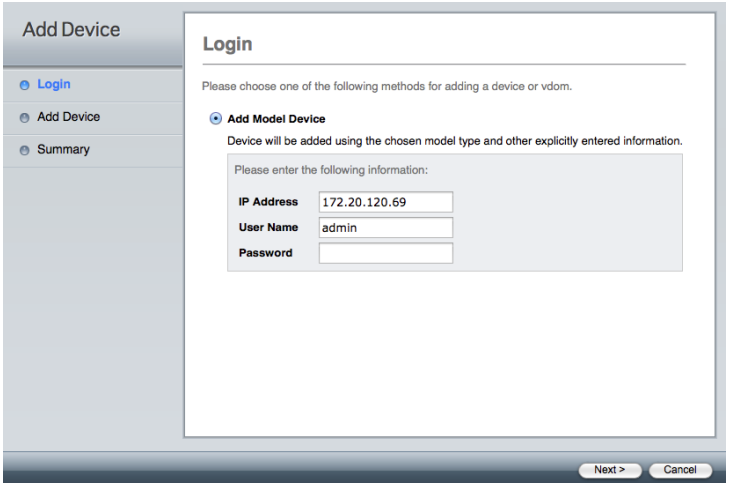
Go to the **Device Manager** tab.

Select **Add Device** from the drop down menu.



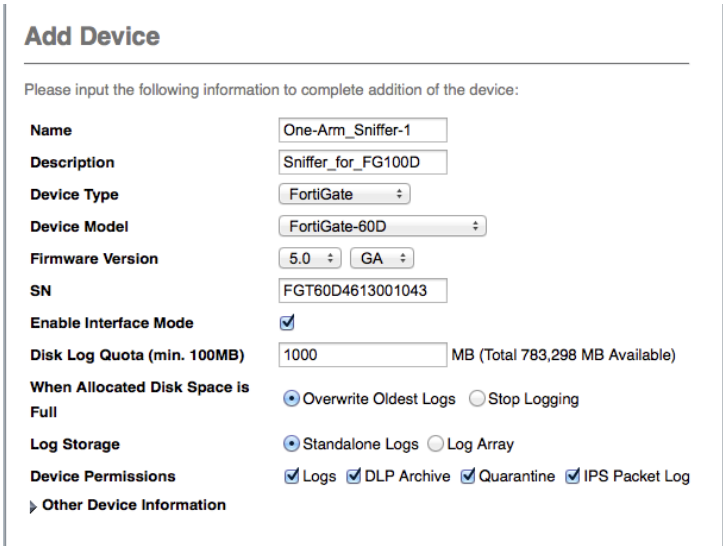
In the **Login** screen of the **Add Device** wizard fill in the fields with the information shown here.

Select **Next**.



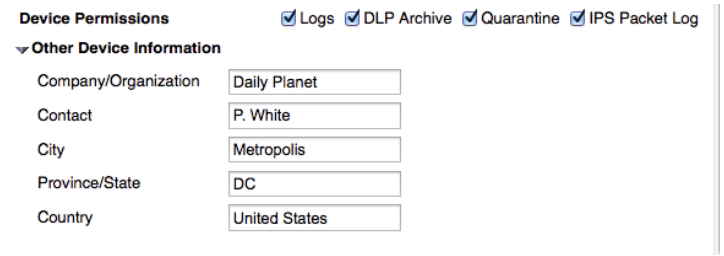
In the **Add Device** screen of the **Add Device** wizard fill in the fields with the information shown here.

If there is no more information to enter, select **Next.**



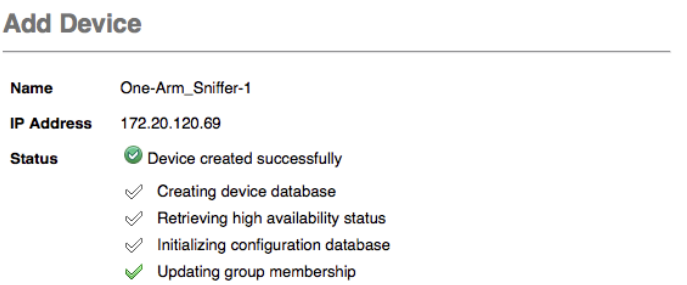
Select the sideways triangle next to **Other Device Information** to expand the window for more field options.

Select **Next.**



A window showing successful registration should appear.

Select **Next** to proceed.



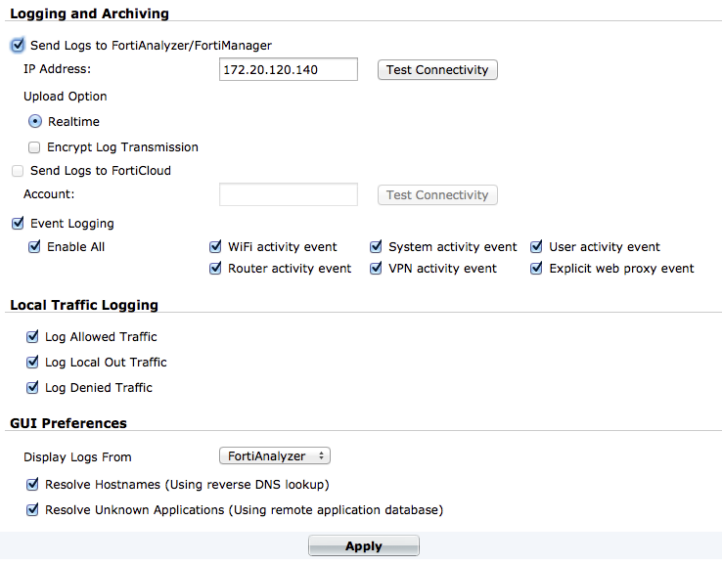
The final window of the wizard provides a summary of the configuration.

Configure logging to the FortiAnalyzer

Go to **Log & Filter > Log Config > Log Settings.**

Configure the settings as shown here.

Be sure to test the connectivity before proceeding.



Results

Creating some logs

On a computer behind the primary FortiGate, download some test files from the Eicar website at:

http://www.eicar.org/85-0-Download.html

Visit some websites that should be blocked by the policy, for example:

www.gambling.com

Seeing the results on the FortiAnalyzer

Log in to the FortiAnalyzer

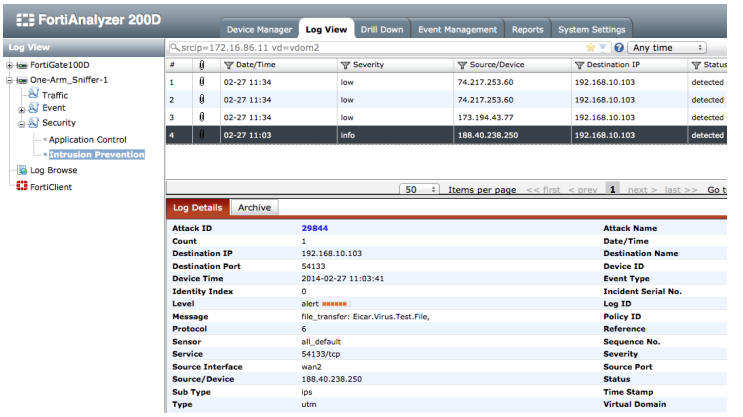
Go to the **Log View** tab.

In the left-hand column, expand the tree for the sniffer device.

Go to **Security > Intrusion Prevention**.

You will see a listing of the items that are considered relevant.

In this case the one for the test file shows the **Attack Name** as Eicar.Virus.Test.File



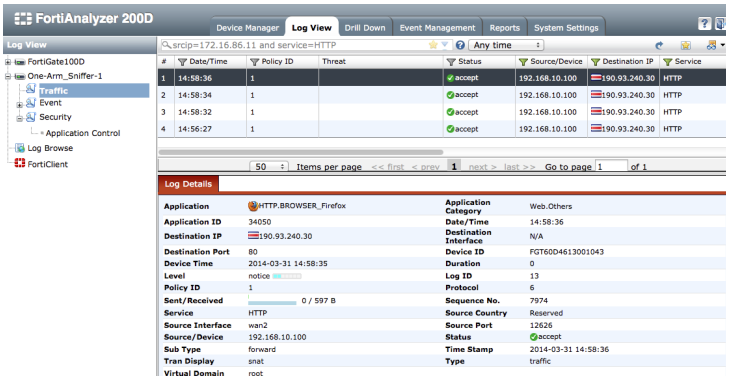
Select the **Log View** Tab.

In the left-hand column, expand the tree for the sniffer device.

Select **Traffic**.

Use the column filters to focus in on the target traffic. In this case we are looking for traffic with:

- Source IP address = 192.168.10.100
- Destination IP address = 190.93.240.30
- Service = HTTP



The destination address was determined by pinging gambling.com and looking at the resolved address.